# Privacy and Personal Information Protection by Social Media Companies in an AI era

**Murdoch Watney**
University of Johannesburg, South Africa

mwatney@uj.ac.za

**Abstract:** Social media platforms have become vast and powerful tools for connecting, communicating, sharing content, conducting business, and disseminating news and information. The history and evolution of social media illustrates not only the digital society's ever-growing dependence on social media, but also the downside to this reliance, namely the challenges of protecting a social media user's privacy and personal information. As technological advancement such as artificial intelligence (AI) grow and impacts on the way data, not only personal but also product and service data, is collected, the spotlight is increasingly focusing on the difficulties in privacy and data protection in an AI-era. The discussion focusses on the misconduct by social media companies in respect of privacy and personal information and the lessons learnt from the way in which social media companies have dealt with social media users' information. Since self-regulation by a social media company does not provide adequate safeguards that privacy and personal information will be protected, limitations to the collection, use, access, and storage of personal information must be imposed by means of legislation. To ensure compliance, non-compliance must be linked to a penalty and enforced by a government. Privacy and data protection regulations were formulated in a pre-AI era, and at that stage, the implications of the rapid evolution of AI on privacy and data protection were not foreseen. To ensure digital trust in an AI era, the legal consequences of misconduct of social media companies must be explored. Social media users must have control of their own data and social media companies must be clear about the kind of data a company will collect on its users, and for what purposes. The lessons learnt from past misconduct is also indicative of whether personal data protection legislation is flexible enough to provide for AI or whether specific legislation must be implemented as society enters the AI era. As the Fourth Industrial Revolution takes shape and AI gains prominence, the data legal landscape is evolving with compliance and enforcement being key to protecting privacy and data, addressing legal uncertainty, and ensuring trust.

**Keywords:** Social media, Social media privacy and personal data protection, Data protection legislation, Legal consequences of social media companies' misconduct in respect of privacy and personal data protection, Impact of AI on social media privacy and personal information protection

## 1. Introduction

Billions of users populate major social networks including Facebook, Instagram, TikTok, Snapchat, YouTube, LinkedIn, and dating apps like Grindr and Tinder. The discussion focuses on the cybersecurity and privacy lessons learnt from social media companies' misconduct in respect of privacy and personal data protection and the relevance of these lessons in an AI era.

Social media refers to websites or applications that support content sharing, user interaction and the exchange of messages within a collaborative framework. Key to social media is sharable content and social interaction. While many platforms support uploading content, social media enables greater engagement and collaboration between users (Streets, 2023). The violation of privacy and personal data protection is a cyberthreat that must be mitigated by means of cybersecurity. Cybersecurity is the protection of internet-connected systems such as hardware, software, and data from cyberthreats.

The major social media platforms are Instagram, Facebook, WhatsApp, TikTok, Twitter, LinkedIn, Pinterest, YouTube, and Snapchat, with Facebook being the largest social media platform. As of July 2023, there were 5,19 billion internet users worldwide and of these 4,88 billion were social media users (Rivera, 2023). Facebook's monthly active users (MAU) in April 2023 totalled 2,989 billion making it the most used social media platform in the world with YouTube coming at a close second with 2,5 billion MAU. Meanwhile, WhatsApp and Instagram landed third at 2 billion MAU (Rivera, 2023). Although the extraordinary growth of social media is welcomed, it has given platforms exceptional access and influence into the lives of users. An immense amount of data is created on these platforms with the consequence that social media companies are able to harvest sensitive data about individuals' activities, interests, personal characteristics, political views, purchasing habits, and online behaviour. Personal data held by social media platforms is also vulnerable to being accessed and misused by third parties, including law enforcement agencies (Electronic Privacy Information Centre, 2024). The discussion focuses on the conduct of social media companies and not on a data breach by a third party.

The history and evolution of social media as discussed at paragraph 2 hereafter lays the groundwork in explaining why privacy and personal data protection within the social media digital environment has become

contentious and will continue to be so as AI advances and impacts on all industries. At paragraph 3 the relevance of protecting privacy and personal data by means of laws are explained. The lessons learnt from the misconduct by social media companies in respect of privacy and personal information protection are explored at paragraph 4. In 2023, AI truly entered our daily lives. At paragraph 5 the impact of AI on social media is discussed by identifying possible risks of AI use by social media companies and whether specific AI legislation should be implemented.

## 2. Overview of the History and Evolution of Social Media in an Electronic Medium

Lile (2023) opines that the origin of social media remains under debate. The discussion focuses on social media within an electronic medium and within this context it could be argued that social media was invented when the first social networking website, Six Degrees, was launched in 1997. The Six Degrees founder, Andrew Weinreich, is known as the father of social networking (Lile, 2023). Weinreich named the first website for social media after the "six degrees of separation" theory, which proposes that everyone in the world is connected to everyone else by no more than six degrees of separation. Although Six Degrees did not last long as its own social networking site and expired in 2001, the idea of an inter-active, inter-connective and collaborative platform set the stage for social media's rapid evolution to come.

Social media began as a desktop or laptop experience but due to technological advancement, such as the expansion of cellular services, social media moved to mobile phones and tablets. The expansion of the capabilities of cellular phones turned it into "smartphones"; and soon high-speed wireless internet became more readily available in homes, businesses, and public spaces. With the advent of social media apps that could run on smartphones, end users could take their communities with them wherever they went. Social media evolved from connecting friends to businesses that took advantage of this new consumer mobility by serving their customers new, simpler methods of interacting by means of social media — and therefore new ways of buying goods and services.

Facebook (now Meta) began to place advertisements on its platform as early as 2006. Twitter (now X) enabled ads in 2010. LinkedIn, Instagram, Pinterest, Snapchat, and TikTok all have attempted to monetize their services through various forms of sponsored advertising. In addition to placing ads on social media platforms, companies discovered the potential utility of cultivating an active, engaged social media presence (Lile, 2023). Whereas social media advertising must be paid for, the act of creating and sharing informative or entertaining content on Meta, Instagram, and other platforms is an attempt by brands to grow an audience organically, in other words, without paying for it directly.

The evolution also shows today's world runs on personalization. It has permeated everyday life, from grocery shopping to reading the news (Mahanakrishnan, 2023). Businesses use every single piece of information they can find about their users to deliver seamless, intuitive solutions. To provide relevant products, services, and information to the users, personal data is stored and processed at multiple levels. Initially social media users found the personalised service convenient, but it soon became apparent that without laws in place that the personal information may be misused, and this resulted in users' mistrust in social media as was seen with the 2018 Cambridge Analytica scandal. At paragraph 4 social media companies' misconduct is discussed.

Social media revolves around information and therefore, the phrase 'data is the new oil' explains the relevance of data (Mahanakrishnan, 2023). This phrase is even more apt now with the advancement and expansion of AI. Data is the lifeblood of AI development. Without data, the algorithms and models that power AI would be unable to learn from past experiences. AI, at its core, leverages machine learning algorithms to process data, facilitate autonomous decision-making, and adapt to changes without explicit human instruction. Technology has pervaded almost every industry, from healthcare to fashion, finance to agriculture, and beyond. As AI technology continues to expand across these industries, it creates a labyrinth of privacy and data protection concerns, thereby challenging traditional norms of personal data protection (Sher and Benchloauch, 2023). Social media users' privacy and personal information must be protected by means of laws and the relevance of protection by means of laws will be explained hereafter at paragraph 3.

## 3. Understanding the Legal Relevance of Social Media Privacy and Data Protection Regulation

### 3.1 Difference Between Privacy and Data Protection

It is important to understand the difference between privacy and personal data protection. Digwatch (2023) explains that privacy and data protection are two interconnected internet governance issues. Privacy must be

scrutinised within the context of personal data protection. Privacy is a fundamental human right and data protection law is the legal mechanism that guards the right to privacy. Privacy is usually defined as the right of any citizen to control their own personal information and to decide whether to disclose information or not. Personal data is any information that can be used to, directly or indirectly, identify a human. Personal data usually comprises name, gender, email address, location information, IP addresses, web cookie information, and biometric data.

### 3.2 United Nations' Recognition of Digital Privacy

The right to privacy is not only recognised in the Universal Declaration of Human Rights but also in the International Covenant on Civil and Political Rights (ICCPR), and in many other international and regional human rights conventions.

As discussed at paragraph 2, social media has evolved since 1997 and will continue to evolve as technology advances. Technological advancements impact on privacy and data protection as huge amounts of data and not only personal data, is collected, accessed, and stored electronically. The appointment of the first United Nations (UN) Special Rapporteur on the Right to Privacy in the Digital Age in July 2015 is a clear indication that the UN considers privacy important as a global digital policy. The UN recognises the necessity to address privacy rights issues on national and global levels.

### 3.3 EU and Global Impact of European Union (EU) GDPR

The EU has taken the lead in protecting privacy and personal data and keeping abreast of technological changes. The General Data Protection Regulation (GDPR) was passed in 2016 after the EU decided to update its existing set of data protection laws that were created in 1998. A 160-page document of 99 articles of law was released. As of May 2018, it is mandated that all relevant organizations be compliant with these laws. The GDPR ensures that all personal data is collected by means of a secure and legal process, with proper consent from the users. It places more power at the user's end and extra responsibility at the business end and this approach enhances the user's digital trust. The GDPR is considered the toughest in the world as far as data privacy, collection, and protection of personal information are concerned (Mahanakrishan, 2023; Wolford, 2023).

What makes the EU GDPR relevant on a global level is that the GDPR – although not issued by the UN – has set an universal standard for personal data protection and many countries have implemented personal data processing protection legislation similar to the GDPR. In 2023, 18 countries outside of the EU has GDPR-like data protection laws (Zafar, 2023). The South African data protection legislation, Protection of Personal Information Act 4 of 2013 (POPIA) which came into operation in July 2022, is based on the GDPR albeit with some differences.

GDPR, which focuses on data security and data privacy, applies to all people residing in EU member states. Although the United Kingdom (UK) departed from the EU as of January 2021, the GDPR was enacted before its withdrawal and is therefore considered a valid UK law. However, the UK will have a domestic data protection shift in 2024. The Data Protection (Fundamental Rights and Freedoms) (Amendment) Regulations (SI) (2023) will amend the UK data protection legislation to refer to rights derived from UK law, rather than retained EU law rights. Provided it is approved by parliament, the SI will come into force at the start of 2024.

All businesses that operate within the EU must be GDPR-compliant. Any company that does not primarily operate in the EU, but still has a part of its user base in the EU needs to comply with this set of laws as well. This means that a South African business will have to comply with the GDPR.

An overview of the provisions of the GDPR is relevant to all countries that have business relations with residents of the EU member countries. The GDPR provides that processing of personal data of a data subject refers to data collection, data storage, data sharing, organizing, analysing, structuring, and deleting. The processing must be done in accordance with seven protection and accountability principles. A data subject is the person whose data is being processed. They are the 'users' — consumers or visitors to a product or a website. A data subject must give consent before any of their personal data is collected or processed. Certain prerequisites must be complied with for the consent requirement to be compliant with the GDPR, such as using clear, plain language and explaining how data is going to be used, why and by whom. Users also have the right to revoke this consent at any time. The data controller is a person, organization, or authority that determines the specifics of data processing. This includes what data is to be collected, who the data subjects are, and how it will be used. The controller also decides how this can be achieved. This is usually a business; for example, a retail chain that wants to provide targeted ads to shoppers. The data controller works alone or with other controllers. The data processer is the third party who does the actual processing based on the input provided by the controller.

Compliance is ensured by means of accountability. Both controllers and processors are liable to fines if they fall short of GDPR standards. At paragraph 5 the GDPR will be compared to the EU AI Act.

## 4. Lessons Learnt From Misconduct by Social Media Companies

The discussion hereafter shows that the misconduct by social media companies have had legal consequences and the legal consequences are also relevant in respect of the impact of AI on social media discussed at paragraph 5.

- Self-regulation of privacy and personal information does not provide adequate protection

In 2018, Facebook acknowledged that it had allowed Cambridge Analytica, a political data mining firm, to access personal information of 87 million Facebook users without the consent of the users. The Cambridge Analytica had far reaching consequences (Harbath and Fernekes, 2023). It focused the attention on various issues, such as the importance of digital trust in the use of AI, the role of social media companies in respect of allowing third party access to information without the consent of the users, the ineffectiveness of self-regulation by social media companies and the role of political adverts.

- Resources: ensuring social media compliance with data protection regulations require resources

In 2020 Germany complained that the Ireland Data Protection Board (DPB) was slow to impose heavy fines on social media companies for non-compliance with the GDPR (Kolbie, 2020). Meta and Google have their European headquarters in Ireland and in terms of the "one stop shop" model, the Ireland DPB is tasked with the investigation into misuse. Ireland DPB has shown a commitment in enforcing compliance of the provisions of the GDPR by imposing heavy fines for non-compliance. In May 2023, the Irish Data Protection Commission (DPC) imposed the largest ever fine of €1,2 billion on Meta, (formerly known as Facebook) the owner of social media platforms such as Instagram and WhatsApp. The fine was issued for the transfer of personal data of European users to the United States (US) without adequate protection. Meta indicated that they plan to appeal the decision (Wessing et al, 2023). Of the top 20 GDPR fines recorded, seven were imposed on Meta or Meta-owned companies. For example, in September 2022, the Data Protection Committee (DPC) levied a fine of €405 million on the company for violating the terms of processing the data of child users on Instagram. Instagram allowed teenagers aged 13-17 to create business accounts on the platform, which made their contact information, such as phone numbers and email addresses, publicly available.

In 2020 Kobie (2020) identified lack of resources such as adequate staff and funding as a key issue in the delay of Ireland DPB for finalising data security and privacy investigations. In 2023, Zafar (2023) reiterated that that the EU's executive arm is severely stretched for resources, funds, expertise, and time. He surmises that this is a huge problem, especially in circumstances in which the EU has to defend its decisions when companies inevitably litigate their penalisation.

The South African Office of Information Regulator (IR) has been criticised for taking a long time in finalising data breaches and it has been alleged that this can be contributed to lack of resources, such as funding, and knowledgeable investigators (Mzekandaba, 2023). If the EU is experiencing resource issues, how much bigger will the issue be in a developing country such as South Africa. A further concern is that if the investigations into personal information misuse by a social media company pose challenges, then the protection of data in the AI era will be even more burdensome.

- Transfer of information between countries: social media companies must ensure adequate protection of social media user's personal information in the transfer of information

The transfer of personal data between countries has been a contentious issue. It must be regulated to provide safeguards for the use, access and storage of personal information. In 2023, the EU and the UK adopted adequacy decisions in relation to data transfers to the United States (US) where importing organisations are signed up to the EU-US Data Privacy Framework (DPF) and UK Data Bridge. US companies will be able to join the EU-US DPF by committing to comply with a detailed set of privacy obligations, for instance the requirement to delete personal data when it is no longer necessary for the purpose for which it was collected, and to ensure continuity of protection when personal data is shared with third parties (European Commission, 2023). Wessing et al (2023) opine that the transfer of personal data between the EU and US may remain contentious in 2024 and that the DPF may be challenged in the European Court of Justice (Wessing et al, 2023).

- Social media companies use of behavioural advertising

Behavioral advertising is a technique used by online advertisers to present targeted ads to consumers by collecting information about their browsing behavior.

In 2023, the European Data Protection Board (2023) issued an instruction to the data regulator of Ireland to impose a permanent ban on Meta for the processing of personal information for behavioural advertising without specific consent from users. Under GDPR, social media users in the EU must give specific consent before they are presented with personalised advertisements.

- Social media companies must provide assurance that sensitive social media users' information will not be accessed by a third party

At the end of 2023 social media lawmakers in the US, EU and Canada have escalated efforts to restrict access to TikTok, the massively popular short-form video app that is owned by the Chinese company, ByteDance, citing security threats. Lawmakers and regulators in the West have increasingly expressed concern that TikTok and its parent company, ByteDance, may put sensitive user data, such as location information, into the hands of the Chinese government. They have pointed to laws that allow the Chinese government to secretly demand data from Chinese companies and citizens for intelligence-gathering operations (Porter, 2023). The 2018 Cambridge Analytica illustrated the importance of ensuring digital trust in social media.

## 5. AI and Social Media

### 5.1 Risks of Social Media Companies Usage of AI Technology

Social media companies are already using generative AI technology. Tshabalala (2023) indicates that AI is changing the social media landscape in the following ways:

- The use of content curation: Social media platforms, such as Facebook and Instagram use AI algorithms to curate content that is most relevant to their users. The algorithms consider factors, such as engagement, behaviour, and interests, to deliver personalised content to users. This has led to an increase in engagement and a more personalised social media experience for users.
- Personalisation: AI algorithms can analyse user data, behaviour, and interests to deliver personalised content, product recommendations, and advertisements.
- Chatbots usage: Chatbots can automate customer service, answer frequently asked questions, and provide real-time support to customers.
- Predictive Analytics: Predictive analytics can analyse social media user behaviour and provide insights into preferences and behaviour. This information can be used to create targeted marketing campaigns, improve customer service, and optimise social media content.

One of the most prominent risks associated with AI in social media is privacy. AI algorithms can analyse vast amounts of user data to create detailed profiles, track user behaviour, and predict their preferences. AI's privacy dilemma rests on a handful of key issues. Firstly, the technology's insatiable appetite for extensive personal data to feed its machine-learning algorithms has raised serious concerns about data storage, usage, and access. Moreover, AI's remarkable capacity to analyse data and make complex analyses amplifies privacy concerns. The technology's potential to infer sensitive information, such as a person's location, preferences, and habits, poses risks of unauthorized data dissemination (Sher and Benchloauch, 2023).

### 5.2 Regulating AI Technology

Self-regulation in the development and use of AI may not be successful and AI may need to be regulated.

At the end of 2023 the European Commission reached a political agreement in respect of the Artificial Intelligence Act (Wessing et al, 2023). The EU is the first body globally to enforce binding rules on AI, and the EU hopes this will help it become the world's go-to tech regulator (Heikklilä, 2023). By becoming the first to formalise rules around AI, the EU retains its first-mover advantage. Much like the GDPR, the AI Act could become a global standard (see paragraph 2). Companies elsewhere that want to do business in the world's second-largest economy will have to comply with the law (Heikklilä, 2023).

A characteristic feature of the AI Act is its so-called "risk-based" approach, which has also become known as the pyramid structure of the AI Act. AI systems will be classified according to the degree of risk they pose to the safety of individuals or fundamental rights (Knibbeler and Zadeh; 2023). Legislators agreed on the unacceptable risk category, which means systems that will be banned. The systems falling under that classification include

those that manipulate human behaviour affecting free will, social scoring, and "certain elements of predictive policing" (Heikklilä, 2023). Emotion-recognition technology in the workplace and school systems will also be prohibited (Heikklilä, 2023). Remote biometric identification in public will be banned with specific exemptions for law enforcement, such as preventing human trafficking, fighting terrorism or finding a missing person.

The AI Act provides for 6 principles that AI systems should follow, namely (Pinto, 2023):

- Human agency and oversight;
- Technical robustness and safety;
- Privacy and data governance and for purposes of our discussion, AI system providers and developers should be designing AI systems with data privacy and data protection in mind. The datasets used to train AI systems should be properly governed;
- Transparency: AI systems should be transparent. AI providers should provide clear information about the system's capabilities and limitations, as well as the data sources used to train it;
- Diversity, non-discrimination, and fairness; and
- Social and environmental well-being.

The regulation imposes legally binding rules requiring tech companies to notify people when they are interacting with a chatbot, or with biometric categorization or emotion recognition systems. It will also require them to label deepfakes and AI-generated content, and design systems in such a way that AI-generated media can be detected. The Act will also require all organizations that offer essential services, such as insurance and banking, to conduct an impact assessment on how using AI systems will affect people's fundamental rights. The AI Act will set up a new European AI Office to coordinate compliance, implementation, and enforcement.

It should be noted that the AI Act differs from the GDPR (Knibbeler and Zadeh, 2023). The AI Act applies to providers, users, importers, and distributors of AI systems in the EU market, regardless of their location. On the other hand, the GDPR applies to controllers and processors processing personal data in the EU or offering goods/services to EU data subjects. The AI Act focuses on AI as a product, and even though the AI Act seeks to implement a "human-centric approach", the AI Act regulates AI rather through the concept of product regulation (Knibbeler and Zadeh, 2023). The GDPR plays a dominant role in the processing of personal information, whereas the protection of product or service data may be regulated by other legislation such as the AI Act or the Data Act of 2023 (Wessing, 2023). For example, developing a large language model such as ChatGPT requires the gathering of vast bodies of text through a process called web scraping. These datasets ingest details scraped from open online sources such as social media profiles. The information may be in the public domain but the gathering must still comply with personal data protection such as the GDPR (McLellan, 2023).

Other countries may consider AI legislation in 2024. The US has been discussing such an Act (Ryan-Mosley et al, 2024). The UK has indicated that it is not considering AI regulation at present. China has had a piecemeal approach to AI regulation by releasing individual pieces of legislation every time a new AI product became prominent, for example one set of legislation for deepfake and one for generative AI. China did indicate in 2023 that an AI law was on its agenda. The African Union is working on an AI strategy and likewise African countries such as Rwanda, Nigeria and South Africa are also working on an AI strategy (Ryan-Mosley et al, 2024). The South African Information Regulator could issue a code of conduct in respect of the use of AI for personal information processing in terms of POPIA (De Wet and Fourie, 2023).

## 6. Conclusion

As society moves forward, it must ensure that the pursuit of technological advancement does not come at the cost of privacy and personal data protection. Sher and Benchloauch (2023) opine that the dialogue on the impact of AI on data privacy is ongoing and complex, necessitating sustained engagement from policymakers, technology developers, and the public to ensure a firm commitment to safeguarding the fundamental rights of individuals. Technological development must be embraced, but AI development cannot go unchecked, and in this regard, the EU AI Act is welcomed. Compliance and enforcement will be key in ensuring digital trust and safeguarding the protection of privacy and personal information by social media companies in an AI era, but this will not be an easy task for governments especially if the relevant resources are not available.

## References

Data Protection Amendment Regulations. (2023); [online] https://www.gov.uk/government/publications/the-data-protection-fundamental-rights-and-freedoms-amendment-regulations-2023.

De Wet, PR. and Fourie, J. (2023) "South Africa: AI and data privacy regulations – the complexities of AI technologies and processing personal information", [online], https://vdt.co.za/popia/south-africa-ai-and-data-privacy-regulations-the-complexities-of-ai-technologies-and-processingpersonal-information/.
Digwatch (2023) "Privacy and data protection"; [online]; https://dig.watch/topics/privacy-and-data-protection.
European Commission. (2023) "Data protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows"; [online]; https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721.
European Data Protection Board (2023); [online]; https://edpb.europa.eu/news/news/2023/edpb-publishes-urgent-binding-decision-regarding-meta_en.
Electronic Privacy Information Center. (2024) "Social Media Privacy"; [online]; https://epic.org/issues/consumer-privacy/social-media-privacy/.
Harbath, K., and Fernekes, C. (2023) "History of the Cambridge Analytica Controversy"; [online]; https://bipartisanpolicy.org/blog/cambridge-analytica-controversy/.
Heikklilä M. (2023) "Five things you need to know about the EU's new AI Act"; [online]; https://www.technologyreview.com/2023/12/11/1084942/five-things-you-need-to-know-about-the-eus-new-ai-act/.
Knibbeler, D. and Zadeh, S. (2023) "International: The interplay between the AI Act and the GDPR"; [online]; https://www.dataguidance.com/opinion/international-interplay-between-ai-act-and-gdpr.
Kobie (2020) "Germany says GDPR could collapse as Ireland dallies on big fines"; [online]; https://www.wired.co.uk/article/gdpr-fines-google-facebook.
Lile, S. (2023) "Complete history of social media"; [online]; https://smallbiztrends.com/2023/08/history-of-social-media.html.
Mahanakrishnan, R. (2023) "What is the GDPR and why is it important?" [online]; https://www.spiceworks.com/it-security/security-general/articles/what-is-gdpr/.
McLellan, L. (2023) "What does artificial intelligence mean for data privacy"; [online]; https://www.omfif.org/2023/08/what-does-artificial-intelligence-mean-for-data-privacy/.
Mzekandaba, S. (2023) "Information watchdog sees data breaches notifications double", [online], https://www.itweb.co.za/content/j5alrMQAJOQMpYQk.
Pinto, T. (2023) "AI principles"; [online]; https://artificialintelligenceact.com/ai-principles/.
Porter, J. (2023) "Tiktok ban: all the news on attempts to ban the video platform"; [online]; https://www.theverge.com/23651507/tiktok-ban-us-news.
Rivera, M. (2023) "30 Social Media Statistics Marketers and Creators Need to Know for 2024"; [online]; https://www.clearvoice.com/resources/social-media-statistics/.
Ryan-Mosley et al. (2024) "What's next for AI regulation in 2024?"; [online]; https://www.technologyreview.com/2024/01/05/1086203/whats-next-ai-regulation-2024/.
Sher, G., and Benchloauch, A. (2023) "The privacy paradox with AI", [online]; https://www.reuters.com/legal/legalindustry/privacy-paradox-with-ai-2023-10-31/.
Streets, M. (2023) "The history and evolution of social media explained"; [online]; https://www.techtarget.com/whatis/feature/The-history-and-evolution-of-social-media-explained.
Tshabalala, A. (2023) "The impact of AI on the future of social media"; [online}; https://www.linkedin.com/pulse/revolutionising-social-media-impact-ai-future-adelaide.
Wessing, T. et al. (2023) "Where will the data flow in 2024"; [online]; https://www.lexology.com/library/detail.aspx?g=c24195a9-20d6-4a1c-8226-bcfc168431c6.
Wolford, B. (2023) "What is GDPR, the EU's new data protection law?"' [online]; https://gdpr.eu/what-is-gdpr/.
Zafar, F. (2023) "Countries with GDPR-like Data Privacy Laws"; (2023); [online]; https://finance.yahoo.com/news/18-countries-gdpr-data-privacy-121428321.html.